

Электронный научный журнал «Век качества» ISSN 2500-1841 <http://www.agequal.ru>

2020, №1 http://www.agequal.ru/pdf/2020/AGE_QUALITY_1_2020.pdf

Ссылка для цитирования этой статьи:

Гомцян О.А., Апибян Р.К. Вычисление и измерение разницы времен при параллельной и последовательной генерации кодов C/A, CM и CL для GPS-спутника // Электронный научный журнал «Век качества». 2020. №1. С. 158-169. Режим доступа: <http://www.agequal.ru/pdf/2020/120012.pdf> (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК: 004.021

Вычисление и измерение разницы времен при параллельной и последовательной генерации кодов C/A, CM и CL для GPS-спутника

*Гомцян Оганес Авакович,
зав. кафедры радиоустройств Института информационных и телекоммуникационных технологий и электроники
Национального политехнического университета Армении
hovhannes.gomcyan@polytechnic.am*

*Апибян Роберт Каренович,
аспирант Института информационных и телекоммуникационных технологий и электроники
Национального политехнического университета Армении
apikyan41@gmail.com*

Аннотация. В навигационной системе GPS для кодировки передаваемых сигналов используются C/A, CM и CL коды. Их главная задача - идентификация сигнала, которая указывает на номер спутника. Эти коды можно разделить на два поколения. C/A коды относятся к старому поколению GPS, а CM и CL относятся к новому поколению. Это означает, что только спутники, которые были добавлены в GPS систему после 2006 г. технически имеют модули для передачи сигналов, которые закодированы CM и CL кодами. Однако генерация кодов и старого, и нового поколений GPS основана на генераторах псевдослучайных чисел. В системе GPS псевдослучайные числа генерируются с помощью линейных регистров сдвига с обратной связью (ЛРСОС), которые подразделяются на два типа: Фибоначчи и Галуа. Процесс генерации выходных данных этих регистров является

последовательным, однако есть методы, которые позволяют генерировать выходные данные параллельно. В данной статье вычисляются и измеряются длительности времен между параллельным и последовательным генерациями C/A, CM и CL кодов, основываясь на методике параллельной генерации LРСОС. Эти измерения помогут понять насколько эффективнее будут работать приемники GPS, которые основаны на параллельных генераторах C/A, CM и CL кодов.

Ключевые слова: GPS, C/A, CM и CL коды, LРСОС, приемник, параллельная генерация, последовательная генерация.

Методика работы линейных регистров с обратной связью

Генерация C/A, CM и CL кодов основана на линейных регистрах с обратной связью. Генератор выходных данных C/A кода основан на двух регистрах LРСОС Фибоначчи и является уникальным для каждого GPS-спутника. Генераторы CM и CL кодов основаны на LРСОС Галуа [1]. Отличия между регистрами Фибоначчи и Галуа проявляется в структурах обратной связи (рис. 1).

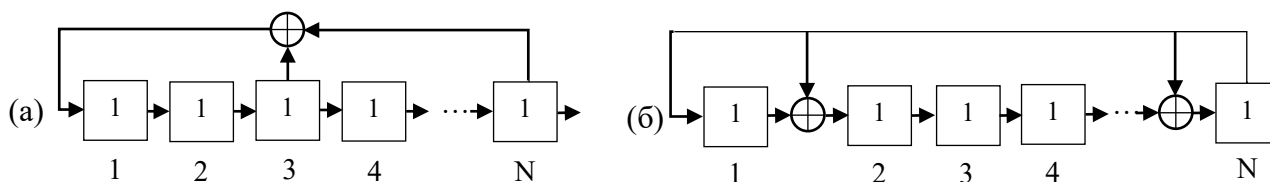


Рис. 1. LРСОС Фибоначчи (а), Галуа (б)

При каждом шаге работы регистра значения битов сдвигаются в правую сторону. Для регистра Фибоначчи (рис. 1-а) значение входного бита является суммой битов по позициям обратных связей. Для рис. 1-а этими позициями являются 3 и N. Для регистра Галуа (рис. 1-б), если в позиции N значение бита равно нулю, то биты регистра сдвигаются в правую сторону без каких-либо изменений, и входной бит является нулем. Если в позиции N битом является единица, то при шаговом сдвиге в позициях обратной связи значения меняются зеркально, что означает, единицы меняются на нули, а нули меняются на единицы и входной бит является единицей. Несмотря на то, что у этих двух типов регистров

входные биты определяются разными методами, у них есть общие характеристики для выходных битов. Так как ЛРСОС составлен из конечного числа битов, то у выходных битов есть цикл повторения. Например, для регистра, который составляется из N -го количество битов, максимальный цикл повторения равняется $m = 2^N - 1$. Однако, цикл повторения не всегда бывает максимальным, для этого регистр должен соответствовать следующим параметрам [2]:

- начальные биты регистра не должны состоять только из нулей, поскольку нули не меняют регистр при сдвиге. Часто начальные биты состоят только из единиц;
- для регистра Фибоначчи количество обратных связей должно быть четным;
- для номеров позиций обратных связей единственным делителем между собой должна быть единица.

Работа ЛРСОС осуществляется последовательно, поэтому для генерации n количества выходных данных необходимо выполнять n -е число сдвигов регистров, что влияет на время, необходимое для процесса корреляции в приемнике. Однако, можно сгенерировать выходные данные регистра параллельно. Для этого нужно вычислить еще не сгенерированные стадии ЛРСОС. Это возможно сделать как для регистра Фибоначчи, так и для регистра Галуа [3]. Ниже представлены формулы для определения будущего состояния регистров Фибоначчи (1) и Галуа (2):

$$S_{i+n} = \oplus \sum_l S_{i+(n-l)} \quad (1)$$

$$S_{i+n} = S_i + \oplus \sum_l S_{i+(l-1)} \quad (2)$$

S – состояние регистра,

i – номер шага сдвига регистра,

n – количество битов в регистре,

l – номер обратной связи.

Для абстрактного представления работы приведенных формул рассмотрим (рис. 2) в случае регистра Фибоначчи, поскольку он является универсальным для обоих регистров.

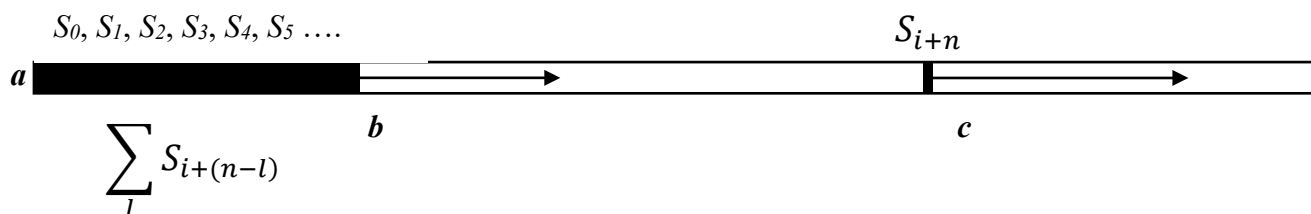


Рис. 2. Абстрактное представление работы формулы (1) для регистра Фибоначчи

Как видно из рис. 2, точка **a** - это начальная стадия регистра. Для расчетов по формуле (1) требуется знания всех состояний до точки **b**, в которой регистр доходит до стадии параллелизации. Это означает, что уже получены все необходимые состояния для расчёта S_{i+n} . Из точки **c**, которая соответствует состоянию S_{i+n} начинается параллельная генерация, причем первый регистр продолжает генерацию из точки **b**, а второй регистр начинает генерацию из точки **c**. Из точки **c** второй регистр генерирует все нужные состояния, чтобы снова применить формулу (1) для регистра Фибоначчи или формулу (2) для регистра Галуа. Таким образом, генерация выходных данных ЛРСОС выполняется параллельно.

Вычисление разницы времен между параллельным и последовательным генерациями выходных битов регистров с обратной связью

Для вычисления разницы времен рассмотрим линейный регистр с обратной связью длиной n битов. Для генерации выходных данных максимального цикла $2^n - 1$, количество параллелизаций регистра равняется $(2^n - 1)/n$.

На рис. 3 показаны первые три шага параллелизации.

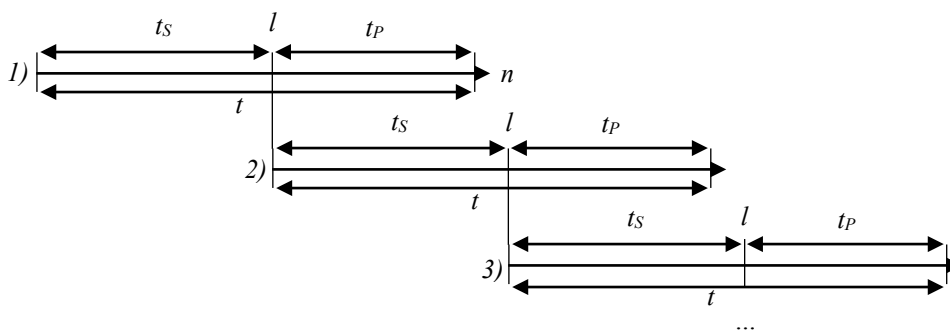


Рис. 3. Первые три шага параллелизации

Обозначим точку параллелизации l , время генерации до точки параллелизации t_s , время после точки параллелизации t_p , а общее время генерации одного шага t . Тогда

$$t = t_s + t_p \quad (3)$$

Во время последовательной процедуры общее время генерации для всего цикла составляет

$$T_s = \left(\frac{2^{n-1}}{n}\right) t \quad (4)$$

Подставив значение t из (3), получим

$$T_s = \left(\frac{2^{n-1}}{n}\right) (t_s + t_p) \quad (5)$$

Можно показать, что общая длительность при параллельной генерации составляет

$$T_p = \left(\frac{2^{n-1}}{n}\right) t_s + t_p \quad (6)$$

Связь между временами генерации t_s , t_p и t можно выразить следующим выражением:

$$t_s = \frac{l}{n} t \quad (7)$$

$$t_p = \frac{n-l}{n} t \quad (8)$$

где l является точкой параллелизации.

Для регистра Фибоначчи точкой параллелизации является $l = (n - l_k)$, где l_k - номер первого регистра обратной связи, а для регистра Галуа $l = (l_k - 1)$, где l_k - номер последнего регистра обратной связи.

Поставив (6) и (7) в формулу (6), получим

$$T_P = \frac{2^{n-1}}{n^2} lt + \frac{n - l_0}{n} t \quad (9)$$

Для сравнения времен между последовательной и параллельной генерациями разделив (4) на (9), получим

$$\frac{T_S}{T_P} = \frac{n2^{n-1}}{l2^{n-1} + n^2 - nl} \quad (10)$$

Расчеты по формуле (10) показывают что время последовательной генерации T_S больше, чем время параллельной генерации T_P .

Абстрактная схема работы параллельного регистра с обратной связью

Как отмечено выше, метод параллельной генерации требует меньше времени, чтобы сгенерировать один цикл выходных данных регистра. Так как ЛРСОС является фундаментальным элементом во многих аппаратных схемах, то ускорение его работы повышает скорость работы генераторов C/A, CM и CL кодов в системе GPS [4].

Генератор C/A кода основан на двух линейных регистрах сдвига с обратной связью, как это показана на рис. 4 [5].

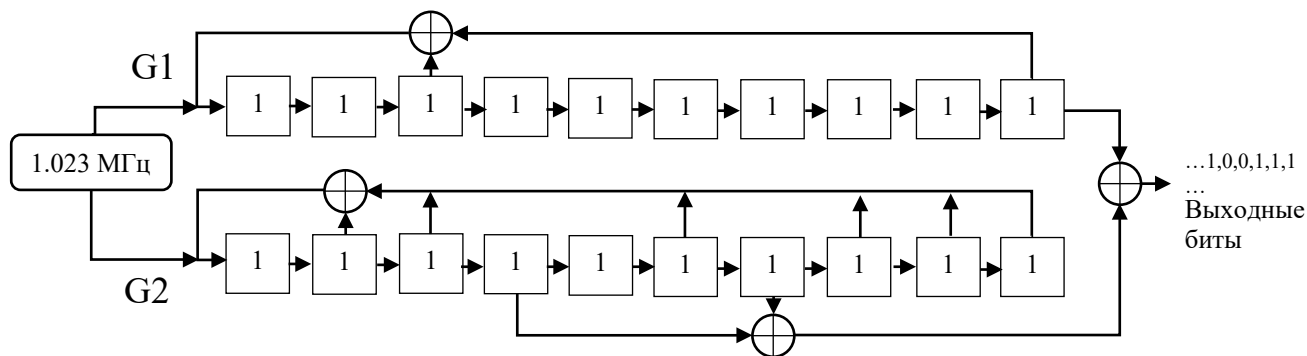


Рис. 4. Схема генератора C/A кода

Как видно из рис. 4, генерация C/A кода основана на двух линейных регистрах Фибоначчи G_1 и G_2 , длина каждого из которых равно десяти. Полиномом регистра G_1 является $1+X^3+X^{10}$, и выходные биты берутся из десятого регистра. Полиномом регистра G_2 является $1+X^2+X^3+X^6+X^8+X^9+X^{10}$, а выходные биты выбираются в соответствие номером спутника из таблицы Роберта Голда, приведённой в [5]. В этом примере выходные данные G_2 выбраны из четвертого и седьмого битов, которые соответствуют двадцатому спутнику. Чтобы сгенерировать C/A код параллельным методом, нужно использовать регистры сдвига, которые будут работать параллельно, используя формулу (1). Поскольку у регистров G_1 и G_2 разные точки параллелизации, то выходные биты генерируются не синхронно, например, G_1 дойдёт до своей первой точки параллелизации на седьмом шагу, а G_2 – на восьмом, и после этого момента синхронизация выходных данных сдвинется по времени.

Для решения проблемы с синхронизацией используется специальный регистр памяти в который попадают выходные биты из G_{P1} и G_{P2} (рис. 5).



Рис. 5. Схема параллельного генератора C/A кода с использованием регистра памяти

Регистр памяти состоит из сегментов. Для каждого выходного бита из G_{P1} и G_{P2} есть свой сегмент в памяти регистра. Работа сегмента состоит в том, чтобы сохранять первый бит из регистров G_{P1} и G_{P2} и сложить его по модулю два со вторым битом (рис. 6).

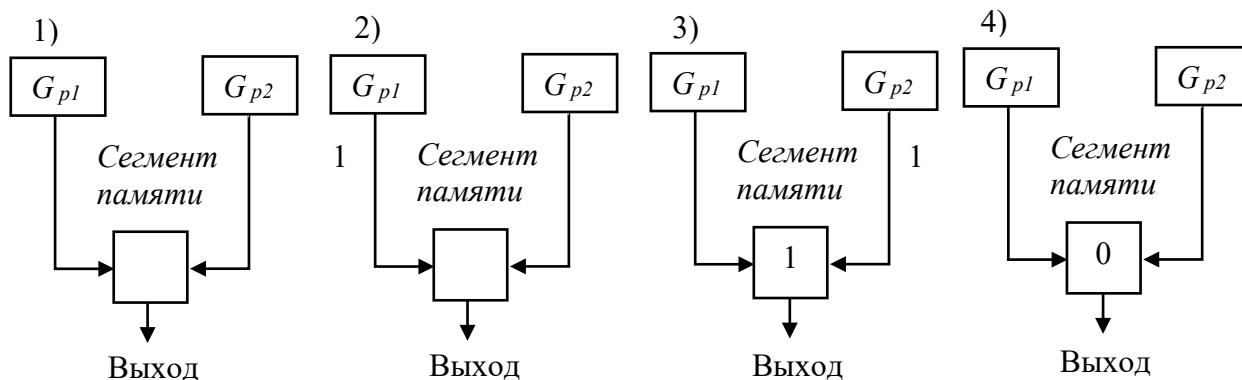


Рис. 6. Стадии работы сегмента регистра памяти

Как показано на рис. 6, сегмент регистра памяти имеет три состояния. В первом состоянии сегмент пуст, так как ни из одного регистра G_{p1} или G_{p2} не поступил выходной бит. Во втором состоянии сегмент получает и сохраняет первый бит от регистра G_{p1} , однако не обязательно, чтобы первый бит поступил от регистра G_{p1} . Третье состояние, когда в сегмент памяти поступает второй бит от G_{p2} регистра и складываются по модулю два со значением первого регистра. Такая методика позволяет выполнить параллельную корреляцию сигналов.

Измерение времени генерации C/A кода

при последовательном и параллельном методах

Для измерения времени генерации применяется программный подход. Разницей между программным и аппаратным подходами в данной задаче является время рекурсии, так как рекурсия при программном подходе занимает больше времени, чем при аппаратном [6]. При аппаратном подходе рекурсия работает быстрее, чем итерация. Сначала мы должны измерить разницу между рекурсией и итерацией для программного подхода, так как процесс параллельной генерации является рекурсивным [7]. В таблице 1 представлены время рекурсии R_T и итерации I_T от количества итераций - n .

Таблица 1. Время рекурсии R_T и итерации I_T в зависимости от количества итераций – n

n	R_T (мс)	I_T (мс)
100	19299	4760
500	97368	7933
1000	166839	11278
5000	742013	43381
8000	1051972	65485

Как видно из таблицы 1, время рекурсии длится намного дольше, чем время итерации. Эти результаты мы будем использовать для корректировок вычислений определение генерации C/A CM и CL кодов.

Для измерения времени генерации C/A кода используется специальная программа, которая вначале фиксирует время старта, а после окончания генерации фиксирует время завершения [8]. Для теста рассмотрим генерацию C/A кода для четырнадцатого спутника. После запуска программы она выдает время параллельной генерации $T_P = 35884819$ мс, а время последовательной генерации $T_S = 3105411$ мс. Как видно из этих результатов, при параллельной генерации быстроедействие не увеличивается из-за отсутствия корректировки в связи с рекурсией и итерацией. Для внесения точности в измерениях надо вычислить коэффициент корректировки для $n=1000$ из таблицы 1 (поскольку один цикл для $n=1024$ времени рекурсии примерно n циклов

$$y = \frac{I_T}{R_T} = \frac{11278}{166839} = 0.067598 \quad (11)$$

Введя корректировку во времени параллельной генерации, получим

$$\frac{T_S}{T_P \times y} = \frac{3105411}{35884819 \times 0.067598} = 1.2 \quad (12)$$

Как видно из (12) параллельная генерация работает в 1.2 раз быстрее, чем генерация C/A кода.

Измерение времени генерации CM и CL кодов последовательным и параллельным методами

В современной GPS системе *CM* и *CL* коды генерируются одним и тем же генератором длиной 27 бит. У обоих кодов полином имеет следующую форму $X^{27}+X^{24}+X^{21}+X^{19}+X^{16}+X^{13}+X^{11}+X^9+X^6+X^5+X^4+X^3+1$ [4]. Расчеты показали, что длительность последовательной генерации для первых 1024 битов составляет $T_S=3135150548$ мс, а при параллельной генерации $T_P=29513449542$ мс. После нормализации измерений получим:

$$\frac{T_S}{T_P \times y} = \frac{3135150548}{29513449542 \times 0.067598} = 1.57 \quad (13)$$

Как видно из (13), генерация кодов *CM* и *CL* параллельным методом работает в 1.57 раз быстрее, чем генерация в последовательном методе [9].

Заключение

В работе получена формула быстродействия между параллельным и последовательным генерациями линейного регистра сдвига с обратной связью. Рассматриваются методы генерации и генераторы псевдо случайных чисел *C/A*, *CL* и *CM* из системы *GPS*. При параллельном методе генерация выходных данных *C/A* кода происходит в 1.2 раз быстрее, чем при последовательном методе, а для *CL* и *CM* кодов - в 1.57 раз быстрее. Отметим, что для дальнейшего повышения быстродействия можно увеличить длину регистров. Весь исходный код программы можно найти в Гид Хабе [10].

Список литературы

1. Goresky M., Klapper A.M. Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers // IEEE (Transactions On Information Theory). 2002. Vol. 48. № 11.

2. Fischer P. Maximum Length Linear Feedback Shift Registers. - URL: https://sus.ziti.uni-heidelberg.de/Lehre/WS1819_DST/LFSR.pdf.
3. Apikyan R. LFSR's Parallel Output Generation. - URL: <https://drive.google.com/file/d/1O6VDb9EiwFnEUGV3DITN5aPd9b7XGpSp/view>.
4. Doberstein D. Fundamentals of GPS Receivers: A Hardware Approach. Springer, 2020. P. 250-260.
5. Bao-Yen Tsui J. Fundamentals of Global Positioning System Receivers: A Software Approach. John Wiley & Sons, Inc., 2000. P. 73-107.
6. Sulov V. Iteration vs Recursion in Introduction to Programming Classes // Кибернетика и информационные технологии. 2016. Т. 16. № 4.
7. Программа для измерения рекурсии и итерации. - URL: https://github.com/RobertApikyan/GpsGenerator/blob/ca_parallel_generation/src/src/main/RecursionVsIteration.java.
8. Программа для параллельной генерации C/A кода. - URL: https://github.com/RobertApikyan/GpsGenerator/blob/ca_parallel_generation/src/src/polynomial/parallelCaGenerator/ParallelCa.java.
9. Программа для генерации CL/CM кодов. - URL: https://github.com/RobertApikyan/GpsGenerator/blob/ca_parallel_generation/src/src/polynomial/parallel_galois_lfsr/GaloisParallelLFSR.java.
10. Ссылка на весь исходный код программы. - URL: <https://github.com/RobertApikyan/GpsGenerator>.

Calculation and measurement of the difference of time of parallel and sequential generation for C/A, CM and CL codes in GPS

Gomtsyan Hovhannes Avakovich,
Head of Radio devices chair.
Institute of information and
telecommunication technologies and electronics
of National polytechnic university of Armenia
hovhannes.gomcyan@polytechnic.am

Apikyan Robert Karenovich
PHD student,
Institute of information and
telecommunication technologies and electronics
of National polytechnic university of Armenia
[*apikyan41@gmail.com*](mailto:apikyan41@gmail.com)

Abstract. The C/A, CM and CL codes are using for broadcasting signal encoding in GPS. Their main task is signal identification, which indicates the number of the satellite from which it was sent. These codes could be divided into two generations. C/A codes refer to the old generation GPS, while CM and CL refer to the new generation, which means that only satellites that were added to the GPS system after 2006 technically have modules for transmitting signals that are encoded with CM and CL codes. However, the generation of codes of the old and new generations of GPS are based on pseudo-random number generators. In GPS, pseudo-random numbers are generated using linear feedback shift registers (LFSR), which are of two types, named by name Fibonacci and Galois. The process of generating the output of these registers is sequential, but there are methods that allow to generate output in parallel. This article computes and measures the time difference between parallel and sequential generations of C/A, CM and CL codes, based on the method of parallel generation of LFSR. These measurements will help to understand how much more efficient GPS receivers will be based on parallel C/A, CM and CL code generators.

Keywords. GPS, C/A, CM and CL codes, LFSR, receivers, parallel generation, sequential generation.